

REMARKS

Information Disclosure Statement

The Action states that two foreign references, CN 1170995A and JP 2002247111, submitted in the IDS's filed on April 18, 2005 and August 10, 2006 were not considered because they lacked English translations. This is incorrect. A translation of the International Search Report, including JP 2002247111, was filed with the application, and was therefore in the file at the time the application was considered on the merits. Further, US Patent No. 6,058,476, the US counterpart to CN 1170995A, was also filed and cited in the IDS filed of August 10, 2006. Applicant respectfully requests that the two noted foreign references be considered and made of record.

Objections to the Specification

The Abstract has been objected to for using legal phraseology. A marked copy and clean copy of substitute abstract are attached to this paper. The abstract has been amended to remove the instances of legal phraseology. Applicant respectfully requests that the objection to the abstract be withdrawn in light of the amendments found in the substitute abstract.

The specification has been objected to for containing reference numerals referencing figures that were not submitted. A marked-up copy and a clean copy of a substitute specification are attached to this paper, striking the objectionable reference numbers. The specification has been amended to remove the reference numerals. Applicant respectfully requests that the objection to the specification be withdrawn in light of the amendments found in the substitute specification.

Application No. 10/531,569
Amendment dated March 11, 2008
Reply to Office Action of December 11, 2007

Applicant(s): Tao ZHANG et al.
Atty. Docket: 46843-216978 RK

Objections to the Claims

Claims 1 and 5 have been objected to for containing informalities. Claim 1 has been amended to remove the phrase “responding to MGC.” Claim 5 has been amended to remove references to “said parameter.” The steps involving “the security authentication parameter” that were in claim 5 have been moved into new claim 6. Claim 6 does not introduce any new subject matter.

Applicant respectfully requests the withdrawal of the objection to claims 1 and 5 in light of these amendments to the claims.

Rejections under 35 U.S.C. § 112

Claim 1 has been rejected under 35 USC 112 for being indefinite, due to lack of antecedent basis for “the security authentication.” The phrase “the security authentication has been amended to be “a security authentication,” and the expression “the authentication result” has been amended to be “the calculation result,” which has an antecedent basis. It is respectfully submitted that claim 1 as amended is definite under 35 USC 112.

Rejections under 35 U.S.C. § 102

Claims 1, 4 and 5 have been rejected under 35 USC 102(e) as being unpatentable over US Patent No. 6,961,857 (Floryanzia). Applicant respectfully traverses these rejections.

Claim 1 has been amended to recite “receiving by the MGC a calculation result obtained

by performing an encryption calculation on the request data using the authentication key by the MG; and determining by the MGC whether the MG is legal according to the calculation result.” The Action aligns MGC of claim 1 with the Gatekeeper of Floryanzia. However, the Gatekeeper of Floryanzia does not perform the step of “determining by the MGC whether the MG is legal according to the calculation result.” Instead, a RADIUS server is used in Floryanzia to determine whether the Gateway is legal, and the RADIUS server then passes its determination back to the Gatekeeper. Claim 1 recites interaction between only the MGC and MG in determining if the MG is legal. Floryanzia requires a third party, the RADIUS server, to perform the authentication of the Gateway for the Gatekeeper.

Claim 1 recites “sending, by the MGC [Media Gateway Controller], security authentication request data to the MG [Media Gateway] using the data package.” Floryanzia does not disclose or suggest this feature of claim 1. Instead, Floryanzia discloses the opposite of claim 1. The Action aligns the Gatekeeper of Floryanzia with the claimed MGC and the Gateway of Floryanzia with the claimed MG. The Access Token in Floryanzia is sent from Gateway to the Gatekeeper, and not the other way around, as claimed. That is, the Gateway in Floryanzia is initiating the registration request. By contrast, in claim 1, the MGC sends the security authentication request to the MG. Because Floryanzia discloses the Gateway initiating the registration request, which is directly opposite to what is claimed, Floryanzia cannot and does not disclose or suggest the recited feature of claim 1 of “sending, by the MGC, security authentication request data to the MG using the data package.”

Further, The Gatekeeper of Floryanzia does not align with MGC of the present claims as

suggested in the Action. According to the description of column 2, lines 31-33 of Floryanzia, the so-called Gatekeeper does not control the Media Gateway. Figure 2A of Floryanzia depicts both a Gatekeeper and an MGC. The Gatekeeper of Floryanzia cannot perform the functions of the MGC of the present claims, as a separate MGC is required in Floryanzia to supplement the Gatekeeper. This indicates that the Gatekeeper of Floryanzia cannot be aligned with an MGC. As can be understood by those skilled in the art that, the Gatekeeper of Floryanzia is a specific network element in the H.323 protocol that provides address translation and call control services to H.323 endpoints. The MGC of the present invention may be responsible for managing multiple Media Gateways (e.g. managing media resources of MGs, managing the resource states of MGs, and managing the states of MGs), for the exchanging IP and PSTN signaling and also for managing and communicating with multiple Signaling Gateways. The Gatekeeper of Floryanzia cannot perform the functions of an MGC as disclosed and claimed, and therefore cannot be aligned with the MGC of the present claims.

Therefore, for at least the above reasons, claim 1 is allowable over Floryanzia.

Claims 4-6 are allowable over Floryanzia for at least being dependent on allowable claim 1.

Rejections under 35 U.S.C. § 103

Claims 2 and 3 have been rejected under 35 USC 103(a) as being unpatentable over Floryanzia in view of US Patent Publication No. 20020120760 (Kimchi).

Claims 2 and 3 are allowable over Floryanzia for at least being dependent on allowable

Application No. 10/531,569
Amendment dated March 11, 2008
Reply to Office Action of December 11, 2007

Applicant(s): Tao ZHANG et al.
Atty. Docket: 46843-216978 RK

claim 1. Kimchi does not supplement the deficiencies of Floryanzia to with respect to the features of claim 1 as discussed above. Therefore, claims 2 and 3 are allowable over Floryanzia in view of Kimchi for at least being dependent on allowable claim 1.

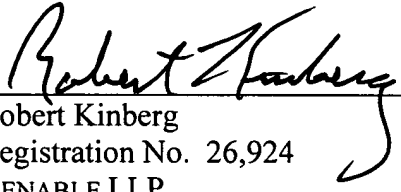
Conclusion

Applicants respectfully request that the Examiner reconsider all presently outstanding rejections and that they be withdrawn in light of the amendments to the claims. Applicants believe that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is hereby invited to telephone the undersigned at the number provided.

Respectfully submitted,

Date:

3/11/08


Robert Kinberg
Registration No. 26,924
VENABLE LLP
P.O. Box 34385
Washington, D.C. 20043-9998
Telephone: (202) 344-4000
Telefax: (202) 344-8300

RK/ish

DC2DOCS/937789

An authentication method for network security includes: configuring a Media Gateway (MG) with an authentication key and setting a security data package on a network protocol by a Media Gateway Controller (MGC); during a security authentication, sending, by the MGC, security authentication request data to the MG using the data package; receiving by the MGC a calculation result obtained by performing an encryption calculation on the request data using the authentication key by the MG; and determining by the MGC whether the MG is legal according to the calculation result. ~~The present invention discloses a authentication method for network security, comprising: firstly, a media gateway controller (MGC) configures a media gateway (MG) with an authentication key and sets a security data package on a network protocol; thus, during the security authentication, the MGC utilizes the security data package to send security authentication request data to the MG; the MG performs an encryption calculation on the request data with the authentication key, and respond to MGC with the encrypted request data; the MGC determines whether the MG being authenticated is legal according to the authenticated result. Said method can prevent illegal or forged devices from accessing to a network; in addition, because that the authentication of MG is performed under the control of MGC, the method is featured with authentication randomness and thereby has higher security authentication efficiency.~~



-1-

AUTHENTICATION METHOD FOR NETWORK SECURITY

Field of the Invention

The present invention relates to an authentication method
5 for network security.

Background of the Invention

In the Next Generation Network (NGN), there are many Media Gateways (MGs) based on Media Gateway Control Protocol (MGCP)
10 or H248 protocol (another Media Gateway Control Protocol, i.e., MeGaCo); these numerous MGs are distributed in enterprises or residences widely, and are featured with covering a wide range, having a great quantity, and being based on dynamic IPs. However, because there being no security authentication mechanism on
15 the application layer of MGCP protocol in the current NGN, the MGs using MGCP protocol are poor in security; though H248 protocol has security authentication mechanism on the application layer, i.e., a security header can be added into each transaction request message of H248 protocol, and the
20 security authentication result can be returned in the transaction response message, but the security authentication mechanism requires exchanging a large amount of H248 messages between MGC and MG, resulting in increasing about 40% time for processing of encoding and decoding H248 messages; thus a
25 security authentication solution provided by conventional H248 protocol severely degrades efficiency of the network system and its feasibility in actual application is poor. Therefore, the problems of system security in the NGN, such as forging MG or attacking to MGC are yet not solved.

–2–

Summary of the Invention

An object of the present invention is to provide an effective authentication method for the NGN security.

5 To attain said object, the authentication method for network security according to the present invention comprises:

step 1: a Media Gateway Controller (MGC) configuring a Media Gateway (MG) with an authentication key, and setting a security data package on a network protocol;

10 step 2: the MGC, during the security authentication, sending security authentication request data to the MG using the data package; the MG performing an encryption calculation on the request data using the authentication key, and responding to MGC with the encrypted request data;

15 step 3: the MGC determining whether the MG being authenticated is legal according to the authentication result.

Said network protocol is Media Gateway Control Protocol (MGCP) or H248 protocol.

20 Said data package comprises: a security authentication request signal and a security authentication completion event; said security authentication request signal comprises a security authentication parameter; said security authentication completion event comprises a security authentication result parameter.

25 Said step 2 further comprises:

step 21: the MGC sending the security authentication request signal in the data package to the MG;

step 22: the MG, after receiving the security authentication parameter in the security authentication

–3–

request signal, performing encryption calculation on said parameter using the authentication key, and reporting the encryption calculated result to the MGC through the security authentication result parameter in the security authentication completion event in the data package.

Since the present invention uses a MGC to configure a MG with an authentication key and sets a network protocol security data package for security authentication of MG, it can prevent network access from illegal or forged devices; in addition, since the authentication of MG is performed under the control of MGC, (in other words, the authentication of MG is performed whenever the MGC considers authentication to be necessary), this kind of authentication has a characteristic of randomness and higher security authentication efficiency.

15

Detailed Description of the Embodiments

Hereunder the present invention will be further described in detail.

The method according to the present invention is for implementing security management of MGs, which in substance comprising: configuring each MG with an authentication key; when initiating an authentication request, a MGC sends a random number to the MG; the MG, according to the random number sent from the MGC and the authentication key configured for the MG (of course, other information may also be included), performs an encryption calculation, and responds to the MGC with the encrypted result. The MGC performs the same calculation to determine whether the encrypted result is identical to that sent from the MG. If not, the MGC will consider the MG as

–4–

illegal.

The present invention may be implemented based on H248 protocol or MGCP protocol, thus a security data package on MGCP or H248 protocol needs to be added; said security data package
5 is a collection of a security authentication signal and an event. The security authentication package on MGCP or H248 protocol employed by the present invention comprises a security authentication request signal and a security authentication completion event. Said security authentication request signal
10 comprises a security authentication parameter. Said security authentication completion event comprises a security authentication result parameter. When the MGC is to perform security authentication of the MG, the MGC sends a security authentication request signal to the MG, and at the same time
15 detects the security authentication completion event from the MG. When the MG receives the security authentication request signal sent from the MGC, it performs an encryption calculation in accordance with the authentication key configured thereon and the parameter in the security authentication request
20 signal. Upon completion of the encryption calculation, the MG reports the security authentication completion event to the MGC, with the security encryption result included in the parameter of the security authentication completion event. When the MGC receives the security authentication completion
25 event from the MG, it compares the encryption calculated result included in the parameter of the reported security authentication completion event with the encryption calculated result calculated by itself, determining whether they are identical or not. If not, the MGC will consider the

–5–

MG as illegal.

Hereunder the above procedures of the present invention are illustrated:

The security data package on MGCP protocol implemented with
5 MGCP protocol as described in the present invention comprises:

Package identifier: Auth; version of data package: 1;

Event included in the data package:

1. Security authentication completion event

Event Identifier: authoc;

10 Event detection parameter identifier: 32*64 (a hexadecimal number);

Note: the event detection parameter is used to return the authenticated result;

Signal included in the data Package:

15 1: Security authentication request signal

Signal identifier: authreq;

Signal parameter identifier: 32*64 (a hexadecimal number, 32 to 64 bits);

The parameter in the security authentication request signal
20 is a random number sent from the MGC to the MG. In this example, the random number is a string, which is longer than 16 bits and shorter than 32 bits. Each string is encoded into 2 hexadecimal numbers through ABNF (Augmented Backus-Naur Form) encoding.

25 The authentication process based on above data package and the pseudo-codes used are:

Step 11: the MGC initiates an authentication request to the MG: the MGC sends a Request Notification (RQNT) command to the MG and allocates Transaction Identifier ~~(100)~~—and

–6–

Request Identifier~~—(123)~~, to request the MG to detect the security authentication completion event (auth/authoc); at the same time, it sends a security authentication request signal (auth/authreq), the MGC generates a 16-byte random
5 number (0x78 0x90 0xab 0xcd 0xef 0x56 0x78 0x90 0x00 0x22 0x00 0x22 0x00 0x22 0x00 0x32) as the security authentication parameter of the security authentication request signal.

Step 12: when receiving the Request Notification (RQNT) command sent from the MGC, the MG returns a correct response
10 to this command (the response code being correct response~~—(200)~~, with the Transaction Identifier ~~(100)~~ identical to that in the Request Notification (RQNT) command sent from the MGC, to acknowledge the MG has received the Request Notification (RQNT) command from the MGC correctly.

15 Step 13: When detecting a security authentication request signal after it receives the Request Notification (RQNT) command from the MGC, the MG begins to perform a security authentication calculation, i.e., performing an encryption calculation with the parameter taken out from the security
20 authentication request signal and the authentication key configured thereon (the authentication key being assumed as 0x12 0x24 0x56 0x78 0x56 0x32 0x78 0x23 0x24 0x25 0x76 0x32 0x32 0x45 0x45 0x32). The result obtained through the encryption calculation is (0x12 0x34 0xab 0xcd 0xef 0xab 0xef
25 0x90 0x00 0x22 0x00 0x22 0x67 0x89 0x77 0x88), the MG generates a security authentication completion event and checks whether the MGC has requested to report the security authentication completion event; if detecting that the MGC has requested to report the event, the MG sends a Notify (NTFY) command to the

–7–

MGC, with the detected event being the security authentication completion event (auth/authoc) and the parameter of the event being the encrypted result. The Request identifier~~—(123)~~ is identical to that in the Request Notification (RQNT) Command
5 sent from the MGC, and the transaction identifier~~—(200)~~ is assigned.

Step 14: when receiving the NTFY command from the MG, the MGC returns a correct response to this command, the response code being correct response~~—(200)~~, with the Transaction
10 identifier~~—(200)~~ being identical to that in the Notify (NTFY) command reported from the MG, to acknowledge the MGC has received the Notify (NTFY) command from the MG correctly.

Step 15: when receiving the encrypted result reported from the MG, the MGC compares the result with the encrypted result
15 calculated by itself; if the two results are identical to each other, the MGC considers the MG as legal; if the two results are not identical to each other or the MG doesn't report the encrypted result within a predefined time, the MGC considers the MG as illegal.

20 The security data package on H248 protocol implemented over H248 protocol according to the present invention comprises:

Package identifier: auth; version of the data package: 1;

Event in the data package:

1: Security authentication completion event

25 Event identifier: authoc (0x0001);

Event detection parameter identifier: authenticated result;

Parameter identifier: Res;

ABNF code of the parameter value: 32*64 (a hexadecimal

–8–

number, 32 to 64 bits);

ASN.1 (abstract symbol notation) code of the parameter
value: OCTET STRING (SIZE (16...32)); (octet of 16 to 32 bits)

Signal included in the data package:

5 1: Security authentication request signal

Signal identifier: authreq

Name of the signal parameter: request parameter;

Parameter identifier: parm;

10 ABNF code of the parameter value: 32*64 (a hexadecimal
number);

ASN.1 code of the parameter value: OCTET STRING (SIZE
(16...32))

The Authentication process based on above data package and
the pseudo-codes used are:

15 Step 21: the MGC initiates an authentication request to
the MG: the MGC sends a Modify command to the MG and allocates
a Transaction Identifier-~~(100)~~ and a Request Identifier-~~(2223)~~,
to request the MG to detect the security authentication
completion event (auth/authoc); at the same time, the MGC sends
20 a security authentication request signal (auth/authreq), and
generates a 16-byte random number (0x78 0x90 0xab 0xcd 0xef
0x56 0x78 0x90 0x00 0x22 0x00 0x22 0x00 0x22 0x00 0x32) as the
security authentication parameter of the security
authentication request signal.

25 Step 22: when receiving the Modify command from the MGC,
the MG returns a correct response to this command, with the
Transaction Identifier-~~(10001)~~ identical to that in the Modify
command, to acknowledge the MG has received the Modify command
from the MGC correctly.

–9–

Step 23: When detecting a security authentication request signal after receiving the Modify command from the MGC, the MG begins to perform a security authentication calculation, i.e., performing an encryption calculation with the parameter
5 taken out from the security authentication request signal and the authentication key configured thereon (the authentication key being assumed as: 0x12 0x24 0x56 0x78 0x56 0x32 0x78 0x23 0x24 0x25 0x76 0x32 0x32 0x45 0x45 0x32). The result obtained through the encryption calculation is (0x12 0x34 0xab 0xcd 0xef
10 0xab 0xef 0x90 0x00 0x22 0x00 0x22 0x67 0x89 0x77 0x88). The MG generates a security authentication completion event and checks whether the MGC has requested to report the encryption completion event; if detecting the MGC has requested to report the event, the MG sends a Notify (NTFY) command to the MGC,
15 with the detected event being the security authentication completion event (auth/authoc) and the event parameter being the encrypted result. The Request Identifier—(2223) is identical to that in the Modify Command sent from the MGC, and the Transaction Identifier—(10002) is assigned.

20 Step 24: when receiving the Notify command from the MG, the MGC returns a correct response to this command, with the Transaction Identifier—(10002) being identical to that in the Notify (NTFY) command sent from the MG, to acknowledge the MGC has received the Notify (NTFY) command from the MG correctly.

25 Step 25: when receiving the encrypted result reported from the MG, the MGC compares the result with the encrypted result calculated by itself; if the two results are identical to each other, it considers the MG as legal; if the two results are not identical to each other or the MG doesn't report the

–10–

encrypted result within a predefined time, it considers the
MG as illegal.